CLAIMS

1. An authentication system comprising:

an access controller operable to communicate with a client via a first communication medium; and,

an authentication server operable to communicate with said client and said access controller via a second communication medium and further operable to generate a first key for delivery to said client and a second key for delivery to said access controller, said second key being complementary to said first key such that when said client and said controller are connected, communications therebetween can be encrypted using said keys; and wherein said access controller is operable to selectively pass instructions received from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met.

2. The authentication system according to claim 1 wherein said first key is a public encryption key and said second key is a private encryption key complementary to said public encryption key.

3. The authentication system according to claim 1 wherein said first communication medium and said second communication medium is selected from the group of networks consisting of the Internet, the PSTN, a local area network, and a wireless network.

4. The authentication system according to claim 1 wherein said computer is a telecommunications switch.

5. The authentication system according to claim 1 wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said first key, a delivery of said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted number using said second key by said access controller, a comparison of said

random number and said decrypted number, and a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number, and a decision not to pass said at least a portion of said instruction if no match is found.

6. The authentication system according to claim 1 wherein said instruction is encrypted by said client using said first key and said verification protocol is based on a successful decryption of said instruction by said access controller using said second key.

7. The authentication system according to claim 1 wherein said first key is only passed to said client after said second key has been successfully passed to said access controller.

8. The authentication system according to claim 1 wherein said first key is only passed to said client if a user operating said client authenticates said user's identity with said server.

9. The authentication system according to claim 1 wherein said access controller contains a preset second key and said server maintains a record of said preset second key; said server operable to only generate said first key and said second key if said access controller successfully transmits said preset second key to said server and said transmitted preset second key matches said server's record thereof.

10. An access controller for intermediating communications between an interface and a computer and operable to store a second key complementary to a first key; said access controller operable to communicate with a client via said interface; said client operable to store said first key and to receive instructions from a user; said access controller operable to selectively pass said instructions to said computer if a verification protocol utilizing said keys is met.

11. The access controller of claim 10 wherein said an access controller is operable to obtain said second key from an authentication server and said client is operable to obtain

said first key from said authentication server, said authentication server operable to generate said first key and said second key.

12. The access controller of claim 10 wherein said first key is a public encryption key and said second key is a private encryption key complementary to said public encryption key.

13. The access controller of claim 11 wherein a medium for connecting said interface and said client is selected from the group consisting of an RS-232 cable, a USB cable, the Internet, the PSTN, a local area network, and a wireless network.

14. The access controller of claim 10 wherein said computer is a telecommunications switch.

15. The access controller of claim 10 wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said first key, a delivery of said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted number using said second key by said access controller, a comparison of said random number and said decrypted number, and a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number, and a decision not to pass said at least a portion of said instruction if no match is found.

16. The access controller of claim 10 said instruction is encrypted by said client using said first key and said verification protocol is based on a successful decryption of said instruction by said access controller using said second key.

17. The access controller of claim 11 wherein said first key is only passed to said client after said second key has been successfully passed to said access controller.

18. The access controller of claim 11 wherein said first key is only passed to said client if a user operating said client authenticates said user's identity with said server.

19. The access controller of claim 11 wherein said access controller contains a preset second key and said server maintains a record of said preset second key; said server operable to only generate said first key and said second key if said access controller successfully transmits said preset second key to said server and said transmitted preset second key matches said server's record thereof.

20. In an authentication server, a method of generating a set of keys for securing access between a client having temporary connection to a computer via an access controller, said access controller for selectively passing instructions received from said client to said computer if a verification protocol utilizing said keys is met, said method comprising the steps of:

receiving a request from said access controller for an updated first key;

authenticating said request;

generating said updated first key and a second key corresponding to said updated first key; and,

delivering said updated first key to said access controller.

21. The method of claim 20 comprising the additional steps of:

receiving a second request from said client for said second key;

authenticating said second request;

delivering said updated first key to said access controller.

22. The method according to claim 20 wherein said first key is a public encryption key and said second key is a private encryption key complementary to said public encryption key.

23. The method according to claim 20 wherein a communication between at least one of said server, said access controller and said client is selected from the group of networks consisting of the Internet, the PSTN, a local area network, and a wireless network.

24. The method according to claim 20 wherein said computer is a telecommunications switch.

25. The method according to claim 20 wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said first key, a delivery of said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted number using said second key by said access controller, a comparison of said random number and said decrypted number, and a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number, and a decision not to pass said at least a portion of said instruction if no match is found.

26. The method according to claim 20 wherein said instruction is encrypted by said client using said first key and said verification protocol is based on a successful decryption of said instruction by said access controller using said second key.

27. The method according to claim 21 wherein said second key is only delivered to said client after said first key has been verified as having been successfully delivered to said access controller.

28. The method according to claim 21 delivered wherein said second key is only passed to said client if a user operating said client authenticates said user's identity with said server.

29. The method according to claim 21 wherein said access controller contains a preset first key and said server maintains a record of said preset second key; said server operable to only generate said first key and said second key if said access controller successfully transmits said preset first key to said server and said transmitted preset first key matches said server's record thereof.

30. A method of securing access between a client and a computer having an access controller intermediate said client and said computer, said method comprising the steps of:

receiving an instruction at said client destined for said computer;

generating a random number by said client;

encrypting said random number by said client using a first key;

delivering said random number, said encrypted random number and said instruction to said access controller;

decrypting of said encrypted number using a second key by said access controller, said second key complementary to said first key;

comparing said random number and said decrypted number;

passing at least a portion of said instruction to said computer if said comparison finds a match of said random number with said decrypted number; and,

discarding said at least a portion if no match is found.

31. An authentication server comprising:

an interface for communicating with a client and an access controller via a communication medium; and

a processing unit operable to generate a first key for delivery to said client and a second key for delivery to said access controller; such that when said controller and said client are connected, said controller selectively passes instructions from said client to a computer attached to said controller if a verification protocol utilizing said keys is met.

32. An authentication server for generating a set of keys for securing access between a client having temporary connection to a computer via an access controller, said

access controller for selectively passing instructions received from said client to said computer if a verification protocol utilizing said keys is met, said server comprising:

means for receiving a request from said access controller for an updated first key;

means for authenticating said request;

means for generating said updated first key and a second key corresponding to said updated first key; and,

means for delivering said updated first key to said access controller.

33. In an access controller for selectively passing instructions between a client and a computer if a verification protocol is met, a method of expiring said verification protocol comprising the steps of:

determining if a first preset period of time since said client disconnected from said access controller has elapsed;

determining if a second preset period of time since said verification protocol was updated has elapsed; and,

expiring said verification protocol by refusing to pass said instructions if either of said preset periods of time have elapsed.

34. The method according to claim 33 wherein said verification protocol utilizes a first encryption key respective to said client and a second encryption key respective to said access controller and said expiring step includes an instruction to said access controller to refuse to accept communications from said client that utilize said first encryption key.